目　录

引言 ……………………………… (3)
1 误差 ……………………………… (3)
1.1 误差的类型与来源 …… (3)
1.2 误差的一些基本概念 … (4)
1.3 误差分析 ……………… (5)
2 插值 ……………………………… (6)
2.1 代数插值的提法及存在唯一性 ……………… (6)
2.2 拉格朗日插值 ………… (7)
2.3 分段线性插值 ………… (8)
2.4 埃尔米特插值 ………… (10)
2.5 三次样条插值 ………… (13)
3 曲线拟合 ……………………… (15)
3.1 曲线拟合及最小二乘原理 …………………………… (15)
3.2 多变量的数据拟合 …… (18)
3.3 用正交多项式作最小二乘拟合 ……………… (19)
4 数值积分与数值微分 ……… (20)
4.1 牛顿-科茨公式、梯形求积公式、抛物线求积公式 … (20)
4.2 复化求积公式 ………… (23)
4.3 逐次分半法 …………… (24)
4.4 理查森外推法和龙贝格求积法 ………………… (25)
4.5 高斯型求积公式 ……… (27)
4.6 数值微分 ……………… (30)
5 常微分方程初值问题的数值解法 …………………………… (31)
5.1 几个常用的定义 ……… (31)
5.2 几种简单的一步法 …… (33)
5.3 龙格-库塔方法 ……… (35)
5.4 线性多步法 …………… (37)
5.5 预估-校正方法 ……… (40)
5.6 常微分方程组和高阶方程初值问题的数值解 …… (41)
5.7 刚性方程组的数值解法 …………………………… (43)
6 常微分方程边值问题的数值解 ………………………………… (44)
6.1 常微分方程边值问题 …………………………… (44)
6.2 打靶法 ………………… (45)
6.3 边值问题的差分解法 …………………………… (46)
7 椭圆型偏微分方程的差分解法 ………………………………… (48)
7.1 椭圆型方程及定解条件 …………………………… (48)
7.2 网格剖分和差分近似 …………………………… (48)
7.3 差分方程组的可解性和收敛性 ………………… (52)
8 抛物型方程的差分解法 …… (53)
8.1 抛物型方程及定解条件 …………………………… (53)
8.2 抛物型方程的差分近似 …………………………… (54)
8.3 几种常用差分格式 …… (56)
8.4 差分格式的稳定性 …… (57)
8.5 差分格式的收敛性 …… (59)
8.6 二维热传导方程混合型问题的差分近似 ……… (61)
9 双曲型方程的差分解法 …… (63)
9.1 双曲型方程及其定解条件 …………………………… (63)
9.2 微分方程的差分近似 …………………………… (64)
9.3 定义、定理和稳定性 … (68)
9.4 对流-扩散方程的差分格式及稳定条件 ……………… (70)
参考文献 ………………………… (71)

目　录

引言 ………………………………（75）
1　求解线性代数方程组的经典算法 ………………………………（75）
1.1　高斯消去法与 *LU* 分解 ………………………………（75）
1.2　矩阵条件数与消去法增长因子 ………………………………（79）
1.3　QR 算法 ………………………………（83）
1.4　经典迭代法及其收敛性 ………………………………（85）
1.5　矩阵求逆与行列式求值 ………………………………（87）
2　求解大型稀疏问题的直接法 ………………………………（88）
2.1　带状矩阵的消去法 ……（88）
2.2　稀疏矩阵的存储 ………（92）
2.3　随机稀疏矩阵的高斯消去法 ………………………（94）
3　求解大型稀疏问题的迭代法 ………………………………（95）
3.1　共轭梯度法 ………………（95）
3.2　不完全因子分解 ………（98）
3.3　GMRES 算法 ………………（99）
3.4　最小二乘问题 ………（101）
4　矩阵特征值问题 ……………（102）
4.1　特征值问题的条件 …（102）
4.2　幂法与反幂法 ………（104）
4.3　雅可比方法 …………（105）
4.4　QR 算法 ………………（107）
4.5　兰乔斯方法 …………（110）
4.6　豪斯霍尔德方法 ……（112）
4.7　广义特征值问题 ………………………（113）
参考文献 ………………………（113）
数学软件 Matlab 介绍 …………（114）

目　录

引言 …………………………… (119)

1 变分原理与剖分插值 ……… (119)

1.1 变分原理 …………… (120)

1.2 剖分插值 …………… (121)

1.3 有限元离散化 ……… (123)

2 协调元的理论分析 ………… (124)

2.1 索伯列夫空间初步 … (124)

2.2 变分问题的适定性 … (126)

2.3 收敛性与误差估计 … (127)

3 其它类型的有限元法 ……… (128)

3.1 非协调有限元法 …… (128)

3.2 混合有限元法 ……… (129)

3.3 无限相似单元法与无限元法 ……………………… (130)

4 经典边界元法 ……………… (131)

4.1 间接边界归化 ……… (131)

4.2 直接边界归化 ……… (133)

4.3 边界积分方程的数值求解 ……………………… (135)

5 自然边界元法 ……………… (136)

5.1 自然边界归化 ……… (136)

5.2 典型区域的自然积分方程 ……………………… (137)

5.3 超奇异积分方程的数值求解 ……………………… (138)

5.4 自然边界元与有限元耦合法 ……………………… (139)

6 自适应有限元边界元法 …… (141)

6.1 自适应有限元法 …… (141)

6.2 自适应边界元法 …… (143)

7 区域分解算法 ……………… (144)

7.1 有限元区域分解算法 ……………………… (144)

7.2 基于边界归化的区域分解算法 …………………… (146)

参考文献 ………………………… (148)

目　录

引言 ………………………… (151)

1 流体力学的基本方程 ……… (151)

1.1 守恒型和非守恒型方程组 ………………………… (151)

1.2 特征理论 ……………… (157)

1.3 间断条件 ……………… (160)

1.4 黎曼问题的解 ………… (161)

2 发展方程的有限差分法 …… (163)

2.1 差分格式的适定性，拉克斯定理 ………… (163)

2.2 差分格式的稳定性分析 ………………………… (166)

2.3 一些常用的差分格式 ………………………… (170)

2.4 多维问题的差分格式 ………………………… (177)

2.5 修正方程及其应用 … (179)

3 可压缩流体流动的差分格式 ……………………………… (182)

3.1 间断、弱解、熵函数、熵通量和熵条件 …… (182)

3.2 伯格方程及其求解 … (184)

3.3 迎风格式 …………… (193)

3.4 TVD 格式 …………… (199)

3.5 ENO 格式 …………… (206)

3.6 气体动力学格式 …… (212)

3.7 时空守恒格式 ……… (225)

3.8 多维问题和 N-S 方程求解 ……………………… (229)

4 不可压缩流体流动的差分格式 ……………………………… (232)

4.1 用投影法解原始变量的 N-S 方程 ……………… (233)

4.2 非错位网格下 N-S 方程的求解 ……………………… (238)

4.3 BGK 法解不可压缩粘性流体流场 …………… (244)

5 高精度格式 ………………… (248)

参考文献 ……………………… (257)

平衡态分布函数矩 …………… (259)

目　　录

引言 ………………………… (265)

1 多重网格法基本原理 ……… (265)

1.1 模型 ……………………… (265)

1.2 多重网格法思想 ………… (266)

1.3 双网格方法 ……………… (267)

1.4 多重网格法原理——一维模型问题分析 …… (269)

2 线性多重网格法 …………… (274)

3 完整的多重网格法 ………… (276)

4 二维多重网格诸元素 ……… (278)

4.1 差分格式 ………………… (278)

4.2 光滑迭代 ………………… (278)

4.3 网格粗化 ………………… (282)

4.4 延拓或插值 ……………… (282)

4.5 限制 ……………………… (284)

5 非线性多重网格法 ………… (285)

5.1 牛顿多重网格法 ………… (285)

5.2 非线性多重网格法 ……… (286)

6 计算机上的执行性能 ……… (290)

6.1 数据结构 ………………… (290)

6.2 存储量 …………………… (291)

6.3 计算量 …………………… (292)

6.4 数值实例 ………………… (292)

参考文献 ……………………… (293)

目　录

引言 ……………………………… (297)

1 预备知识 ……………………… (297)

1.1 与迭代法有关的概念 ……………………………… (297)

1.2 索伯列夫空间及其性质 ……………………………… (299)

1.3 有限元空间及性质 … (300)

2 非重叠区域分解法 ………… (301)

2.1 两子域情形 ………… (301)

2.2 多子域情形 ………… (304)

2.3 界面预条件子的构造 ……………………………… (307)

2.4 非重叠区域分解预条件子 ……………………………… (311)

2.5 非协调情形 ………… (313)

2.6 无界区域问题 ……… (316)

3 重叠区域分解法 …………… (318)

3.1 两子域情形 ………… (318)

3.2 组合网格方法 ……… (321)

3.3 多子域情形 ………… (323)

3.4 变分不等式问题 …… (326)

3.5 非对称、非正定问题 ……………………………… (328)

4 抛物问题的拉格朗日乘子区域分解法 ……………………………… (329)

4.1 基本算法 …………… (330)

4.2 界面矩阵的条件数估计 ……………………………… (332)

4.3 界面预条件子的构造 ……………………………… (337)

参考文献 ……………………………… (342)

目　录

引言 ……………………………… (347)
1　小波分析基础 ………………… (347)
1.1　信号的时频局部化分析 ……………………………… (347)
1.2　连续小波变换 ………… (348)
2　离散小波变换与小波框架 ……………………………… (351)
2.1　离散小波变换 ………… (351)
2.2　框架 …………………… (352)
2.3　小波框架 ……………… (354)
3　多尺度分析与正交小波基 ……………………………… (355)
3.1　多尺度分析与正交小波基的构造 ………………… (355)
3.2　信号的小波分解与合成，Mallat 算法 ……………… (360)
4　紧支集正交小波基 ………… (362)
4.1　双尺度方程的具紧支集解 ……………………………… (362)
4.2　$\varphi(t)$成为尺度函数的条件 ……………………………… (364)
5　小波包 ……………………… (365)
5.1　小波包的构造 ………… (365)
5.2　信号的小波包基展开 ……………………………… (366)
5.3　最优基的选择 ………… (367)
参考文献 ………………………… (368)

目　录

引言 ……………………………… (371)

1　有向网 ……………………………… (371)

1.1　有向网结构 ………… (371)

1.2　网操作 ……………… (374)

1.3　无向网和网拓扑 …… (374)

2　网系统 ……………………………… (376)

2.1　变迁规则 …………… (376)

2.2　基本网系统 ………… (377)

2.3　库所/变迁系统 ……… (378)

2.4　高级网系统 ………… (381)

2.5　自控网系统 ………… (387)

3　同步论与并发公理 ………… (389)

3.1　同步论概念 ………… (389)

3.2　条件/事件系统 ……… (391)

3.3　同步论 ……………… (392)

3.4　并发公理 …………… (395)

4　网逻辑 ……………………………… (398)

4.1　C/E 系统的网逻辑结构 ……………………………… (398)

4.2　推理 ………………… (399)

4.3　P/T 系统和多值逻辑 ……………………………… (400)

5　信息流结构 ……………………… (401)

5.1　基本信息流图 ……… (401)

5.2　信息流图的有向网表示 ……………………………… (403)

5.3　信息元件:一位噪音通道 ……………………………… (404)

参考文献 ……………………………… (404)

目　录

引言 ……………………………… (407)
0 图的几种表示形式 …………… (407)
1 最短路问题 …………………… (409)
1.1 最短路问题的数学模型 ……………………………… (409)
1.2 非负权网络中最短路算法 ……………………………… (410)
1.3 无回路网络中最短路算法 ……………………………… (411)
1.4 无负回路网络中最短路算法 ……………………………… (412)
1.5 所有点对间的最短路算法 ……………………………… (413)
1.6 最短路的变种 ……… (416)
2 最大流问题 …………………… (417)
2.1 最大流的基本概念 … (417)
2.2 最大流算法 ………… (418)
2.3 具有上下界容量网络的最大流 ……………… (422)
2.4 可行性定理及其应用 ……………………………… (423)
3 最小费用流 …………………… (425)
3.1 最小费用流的模型及解的性质 ……………… (425)
3.2 最小费用流的最小平均圈算法 ………………… (427)
3.3 最小费用流的最短路算法 ……………………………… (430)
3.4 最小费用流的网络单纯形算法 ………………… (431)
3.5 最小费用流的 OK 算法 ……………………………… (433)
4 最优树与树形图 ……………… (436)
4.1 树的基本概念 ……… (436)
4.2 最优支撑树 ………… (436)
4.3 第 k 最小权支撑树 … (440)
4.4 最小比例树与最均匀树 ……………………………… (440)
4.5 最优树形图 ………… (441)
4.6 最优划分限制支撑树 ……………………………… (444)
4.7 网络上的施泰纳树 … (446)
5 网络中的选址问题 …………… (449)
5.1 网络的重心 ………… (449)
5.2 网络的中心 ………… (451)
5.3 网络的形心 ………… (452)
5.4 离散的多场址问题 … (453)
6 网络中的最优匹配 …………… (454)
6.1 基本概念 …………… (454)
6.2 最大基数匹配算法 … (454)
6.3 最大权匹配 ………… (456)
6.4 中国邮递员问题 …… (458)
7 网络中的逆最优化问题 …… (460)
7.1 线性规划的逆问题 … (460)
7.2 两类特殊逆线性规划的解 ……………………………… (463)
7.3 逆最短路、指派和最小割问题 ………………… (464)
7.4 逆最小费用流问题 … (466)
7.5 逆最小支撑树问题 … (466)
参考文献 ………………………… (467)

目　录

引言 ………………………… (471)

1 电路网络图 ………………… (471)

1.1 广义的基尔霍夫定律 ………………………… (471)

1.2 状态变量法 ………… (478)

1.3 状态变量法的补充 … (497)

2 信号流图 ………………… (504)

2.1 玛逊信号流图 ……… (504)

2.2 信号流图的运算规则 ………………………… (507)

2.3 科特斯方法 ………… (514)

2.4 玛逊定理 …………… (519)

参考文献 ……………………… (525)

目　　录

引言 ……………………………… (529)
1 随机算法的计算模型 ……… (529)
1.1 蒙特卡罗法和拉斯维加斯法 ……………………………… (529)
1.2 概率图灵机和概率计算复杂性类 …………… (530)
2 指纹术 ……………………… (533)
2.1 指纹术 ………………… (533)
2.2 多项式恒等检测 …… (533)
2.3 模式匹配 …………… (534)
3 素数判定 …………………… (535)
3.1 预备知识 …………… (535)
3.2 索罗维-斯特拉逊算法 ……………………………… (536)
3.3 拉宾算法 …………… (537)
4 图论算法 …………………… (538)
4.1 最小割集 …………… (538)
4.2 最小生成树 ………… (539)
4.3 最大割集的随机近似算法 ……………………………… (540)
5 几何算法 …………………… (542)
5.1 平面上的凸包 ……… (542)
5.2 对偶性 ……………… (543)
5.3 半空间的交 ………… (544)
5.4 德劳赖三角剖分 …… (545)
6 随机并行算法 ……………… (546)
6.1 随机并行排序算法 … (546)
6.2 极大独立集 ………… (549)
6.3 图的匹配 …………… (550)
7 去随机算法 ………………… (553)
7.1 压缩样本空间法 …… (553)
7.2 条件概率法 ………… (554)
7.3 格点近似问题 ……… (555)
7.4 极大独立集的去随机并行算法 …………… (558)
参考文献 …………………… (559)

目　录

引言 ……………………………… (563)
1 概论 ……………………………… (563)
2 优先策略 ……………………………… (565)
2.1 求最短树的库鲁斯卡算法 ……………………………… (565)
2.2 求最短树的普林蒙算法 ……………………………… (566)
2.3 求最短路径的戴克斯徒拉算法 ……………… (567)
2.4 磁带问题 ……………… (569)
2.5 有期限的任务安排 … (570)
2.6 哈佛曼树 ……………… (571)
3 分治策略 ……………………………… (575)
3.1 典型例子 ……………… (575)
3.2 斯徒拉逊矩阵乘法 ……………………………… (576)
3.3 布尔矩阵乘法 ……… (578)
3.4 维纳格拉德算法 ……………………………… (579)
4 动态规划 ……………………………… (580)
4.1 典型问题 ……………… (580)
4.2 最佳原理 ……………… (581)
4.3 流动推销员问题 …… (583)
4.4 矩阵链乘问题 ……… (584)
4.5 最长公共子序列 …… (585)
4.6 应用举例 ……………… (587)
5 搜索技术 ……………………………… (591)
5.1 概述 ……………………… (591)
5.2 无向图的 DFS 算法 … (592)
5.3 有向图的 DFS 算法 … (594)
5.4 BFS 算法 ……………… (596)
5.5 α-β 剪枝术 ……………… (597)
5.6 流动推销员问题的分支定界法 ……………… (597)
5.7 同顺序加工任务安排 ……………………………… (602)
6 FFT 并行算法与脉动阵列 ……………………………… (603)
6.1 并行计算概念 ……… (603)
6.2 FFT ……………………… (604)
6.3 脉动阵列的并行计算装置 ……………………………… (610)
7 排序与查找 ……………………… (611)
7.1 排序的下界估计 …… (611)
7.2 归并排序算法 ……… (612)
7.3 快速排序算法 ……… (613)
7.4 堆集排序算法 ……… (616)
7.5 排序网络 ……………… (620)
7.6 最佳二分树 ………… (622)
7.7 2-3 树 ………………… (626)
8 计算复杂性理论 ……………… (627)
8.1 概述 ……………………… (627)
8.2 图灵机 ………………… (628)
8.3 多项式归约 ………… (631)
8.4 可满足性问题及库克定理 ……………………………… (632)
8.5 若干 NP 完全问题及其证明 ……………………………… (636)
8.6 复杂度类 ……………… (639)
参考文献 ……………………………… (640)

目　　录

引言 …………………………… (643)

1　贪婪算法 ……………………… (643)

1.1　贪婪算法 ……………… (643)

1.2　拟阵 …………………… (647)

1.3　贪婪的启发式算法 … (648)

2　组合最优化的近似算法 …… (649)

2.1　近似算法的性能 …… (649)

2.2　流动推销员问题的近似算法 ………………………… (651)

2.3　装箱问题的近似算法 ………………………… (654)

2.4　0-1 背包问题的近似算法 ………………………… (656)

2.5　0-1 多背包问题的近似算法 ………………………… (658)

3　NP 难问题的可近似性 …… (660)

3.1　不可近似性 ………… (660)

3.2　可近似性分类 ……… (660)

3.3　问题的可近似性一览表 ………………………… (660)

4　局部搜索算法 ………………… (666)

4.1　局部搜索算法的一般描述 ………………………… (666)

4.2　流动推销员问题的局部搜索算法 …………… (668)

4.3　图的均匀划分的局部搜索算法 ………………… (669)

4.4　n 后问题的局部搜索算法 ………………………… (672)

4.5　可满足性问题的局部搜索算法 ………………… (674)

参考文献 ………………………… (676)

目　　录

引言 ………………………………（679）
1　遗传算法 ……………………………（679）
1.1　表达方式 ………………（680）
1.2　处理约束条件 ………（681）
1.3　初始化过程 …………（682）
1.4　评价函数 ………………（683）
1.5　选择过程 ………………（684）
1.6　交叉操作 ………………（684）
1.7　变异操作 ………………（685）
1.8　遗传算法程序 ………（686）
2　遗传算法与上升法的比较 ……………………………………（686）
3　几个应用问题 ………………（693）
3.1　运输问题 ………………（693）
3.2　流动推销员问题 ……（695）
3.3　统计问题 ………………（697）
参考文献 …………………………（700）

目　　录

引言 …………………………… (705)
1　物理学中的模拟退火 ……… (705)
1.1　退火的概念 ………… (705)
1.2　统计物理学基础 …… (705)
1.3　米特罗波利斯准则 … (707)
2　优化中的模拟退火算法 …… (707)
2.1　优化问题 …………… (707)
2.2　局部搜索法 ………… (708)
2.3　从局部搜索法到模拟退火算法 …………… (709)
3　收敛性定理与统计理论 …… (710)
3.1　基本定义 …………… (710)
3.2　基本定理 …………… (711)
3.3　更精确的收敛性定理 ………………………… (712)
3.4　统计特性 …………… (713)
4　冷却进度表 ………………… (715)
4.1　冷却进度表的一般概念 ………………………… (715)
4.2　冷却进度表的确定 … (715)
5　模拟退火算法的应用 ……… (718)
5.1　流动推销员问题 …… (718)
5.2　最大割问题(MCP 问题) ………………………… (719)
5.3　0-1 背包问题(ZKP 问题) ………………………… (720)
5.4　独立集问题(ISP 问题) ………………………… (720)
5.5　调度问题(SCP 问题) ………………………… (721)
5.6　划分问题(PAP 问题) ………………………… (722)
5.7　布局问题(PLP 问题) ………………………… (723)
5.8　图的着色问题(GCP 问题) ………………………… (724)
参考文献 …………………… (725)

目　录

引言 ………………………… (729)
1 构造性代数几何 …………… (730)
1.1 吴-Ritt零点分解算法 ………………………… (730)
1.2 复数域上的投影定理 ………………………… (734)
1.3 代数簇的各种表示及转换 ………………………… (736)
1.4 奇异曲面的陈省身示性类 ………………………… (739)
2 构造性微分代数几何 ……… (742)
2.1 微分域上的吴-Ritt零点分解定理 …………… (742)
2.2 微分域上投影定理 … (744)
2.3 偏微系统的完全可积理论 ………………………… (745)
2.4 微分几何与力学中的定理证明与发现 ………… (747)
3 构造性实代数几何 ………… (749)
3.1 实闭域上的量词消去理论 ………………………… (749)
3.2 多项式的完全判别系统 ………………………… (752)
3.3 构造性实代数几何的应用 ………………………… (754)
4 代数方程组求解算法与应用 ………………………… (755)
4.1 代数方程组求解算法 ………………………… (755)
4.2 杨振宁-柏克斯特方程与量子群 ……………… (760)
4.3 微分系统稳定性与极限环的个数 ……………… (761)
4.4 一类发展方程的行波解 ………………………… (763)
5 几何自动推理的代数方法 ………………………… (766)
5.1 几何定理机器证明的吴方法 ………………………… (766)
5.2 几何公式的自动推导 ………………………… (769)
5.3 面积方法与可读证明自动生成 ………………… (770)
5.4 其它几何定理证明方法 ………………………… (772)
5.5 智能几何软件《几何专家》 ………………………… (772)
参考文献 ……………………… (774)

目　　录

引言 …………………………… (781)
1　符号计算的特征与软件工具 …………………………… (781)
1.1　符号计算的特征 …… (782)
1.2　精确计算和软件工具 …………………………… (783)
1.3　精化算法:符号计算软件的发动机 …………… (785)
2　多项式理想与 Gröbner 基 …………………………… (786)
2.1　理想成员的判定 …… (787)
2.2　Gröbner 基的性质和应用 …………………………… (789)
3　符号计算中的一些关键技术 …………………………… (791)
3.1　结式及迪克森结式 …………………………… (791)
3.2　根的分离与斯特姆序列 …………………………… (794)
3.3　模运算与中国剩余定理 …………………………… (795)
3.4　多项式的因式分解 …………………………… (797)
参考文献 …………………………… (798)

目　录

引言 ………………………………（803）
1 归结方法 ………………………（803）
1.1 前束范示 ……………………（804）
1.2 斯科伦函数 …………………（804）
1.3 子句及子句集 ………………（804）
1.4 基本归结 ……………………（804）
1.5 一阶逻辑的归结 ……………（805）
2 自然演绎 ………………………（811）
3 表格法 …………………………（813）
4 关于带等词的定理证明 ……（814）
4.1 关于等号公理 ………………（814）
4.2 调换 …………………………（814）
4.3 超调换与输入调换 ……………………………（815）
4.4 单元调换与线性调换 ……………………………（815）
5 重写规则 ………………………（815）
参考文献…………………………（817）

目　　录

引言 …………………………… (821)
1　并行计算的模型与算法 …… (823)
1.1　并行计算机结构和模型 …………………………… (823)
1.2　性能和可扩展性的测度 …………………………… (829)
1.3　快速排序的并行算法设计和分析 ……………… (830)
1.4　FFT 的并行算法设计和分析 …………………………… (838)
1.5　评述 …………………… (843)
2　分布计算的模型与算法 …… (845)
2.1　模型 …………………… (846)
2.2　典型算法 ……………… (863)
参考文献 ………………………… (871)

目　录

引言 …………………………… (875)
1 曲线、曲面基础 ……………… (875)
1.1 曲线、曲面的表示 …………………………… (875)
1.2 数据点列的参数化 … (878)
1.3 调配函数 ……………… (879)
1.4 曲线、曲面间的几何连续性 …………………… (883)
1.5 有理参数多项式曲线与齐次坐标 ……………… (887)
1.6 参数曲线、曲面的重新参数化 ………………… (888)
1.7 曲线、曲面的光顺性 …………………………… (889)
1.8 张量积曲面 ………… (896)
2 常用的参数曲线、曲面 …… (897)
2.1 三次参数样条曲线、曲面 …………………………… (897)
2.2 贝齐尔曲线 ………… (901)
2.3 B样条曲线、曲面 …… (908)
2.4 NURBS曲线、曲面 …… (917)
2.5 孔斯曲面 …………… (925)
2.6 等距曲线和曲面 …… (930)
2.7 三角域上的曲面表示 …………………………… (933)
2.8 常用参数曲线、曲面的等价表示 …………… (936)
2.9 扫描曲面 …………… (938)
2.10 基于三维散乱数据的曲面拟合 ………………… (940)
参考文献 ………………………… (946)

目　录

引言 …………………………… (949)
1　几何查找 ……………………… (949)
1.1　点定位问题 ………… (949)
1.2　范围查找问题 ……… (952)
1.3　判定点集是否在多边形内 …………………………… (955)
2　多边形 ………………………… (955)
2.1　凸多边形 …………… (955)
2.2　多边形 ……………… (957)
2.3　多边形的三角剖分 … (958)
2.4　多边形的凸划分 …… (959)
3　凸壳 …………………………… (960)
3.1　凸壳的基本概念 …… (960)
3.2　计算凸壳的算法(二维) …………………………… (961)
3.3　凸壳的应用 ………… (962)
4　沃罗诺图及其应用 ………… (964)
4.1　沃罗诺图的基本概念 …………………………… (964)
4.2　构造沃罗诺图的算法 …………………………… (965)
4.3　平面点集的三角剖分 …………………………… (967)
4.4　沃罗诺图的应用 …… (968)
5　几何体的交 …………………… (969)
5.1　线段相交的算法 …… (969)
5.2　凸多边形的交 ……… (971)
5.3　半平面的交及其应用 …………………………… (972)
6　矩形几何 ……………………… (974)
6.1　矩形几何问题的特征及解决问题的途径 … (974)
6.2　矩形并的面积与周长 …………………………… (975)
6.3　矩形的交 …………… (977)
7　几何体的排列 ………………… (980)
7.1　基本概念 …………… (980)
7.2　确定直线排列的算法 …………………………… (981)
7.3　应用 ………………… (982)
8　算法的运动规划 ……………… (984)
8.1　最短路径 …………… (985)
8.2　移动圆盘 …………… (987)
8.3　平移凸多边形 ……… (988)
参考文献 ……………………… (990)

目　录

引言 …………………………… (993)
1 线性分组码 …………………… (993)
1.1 基本概念 …………… (993)
1.2 标准阵和伴随式译码………………………… (995)
1.3 汉明码 ……………… (996)
2 非线性码 ……………………… (996)
2.1 码的一些界 ………… (996)
2.2 阿达马码 …………… (997)
3 循环码 ………………………… (998)
3.1 循环码的描述 ……… (998)
3.2 循环码的检错能力 … (999)
3.3 循环码的编码 ……… (999)
3.4 循环码的译码 ……… (999)
4 BCH 码 ……………………… (1001)
4.1 BCH 码的定义 ……… (1001)
4.2 BCH 码的译码算法 ………………………… (1001)
5 MDS 码 ……………………… (1003)
5.1 MDS 码的奇偶校验矩阵和生成矩阵 ………… (1003)
5.2 MDS 码的重量分布 ………………………… (1003)
5.3 MDS 码与有限射影几何 ………………………… (1003)
6 R-S 码 ………………………… (1004)
6.1 R-S 码的定义 ……… (1004)
6.2 R-S 码的编码 ……… (1005)
6.3 R-S 码的译码 ……… (1005)
6.4 R-S 码的应用 ……… (1006)
7 交错码 ……………………… (1007)
7.1 交错码的定义 ……… (1007)
7.2 交错码的译码 ……… (1007)
7.3 Goppa 码 …………… (1008)
7.4 广义 Srivastava 码 …… (1009)
7.5 Chien-Choy 广义 BCH 码 ………………………… (1010)
8 R-M 码 ……………………… (1010)
8.1 r 阶 R-M 码 ………… (1011)
8.2 一阶 R-M 码 ………… (1011)
8.3 二阶 R-M 码 ………… (1012)
9 二次剩余码 ………………… (1013)
9.1 二次剩余码的定义 ………………………… (1013)
9.2 二次剩余码的幂等元和生成矩阵 …………… (1013)
9.3 二次剩余码的译码 ………………………… (1014)
9.4 Golay 码……………… (1015)
10 代数几何码 ……………… (1016)
10.1 代数几何码的构造 … (1016)
10.2 代数几何码的重量谱 ……………………… (1017)
10.3 代数几何码的译码 … (1017)
10.4 椭圆码 …………… (1019)
10.5 Hermitian 码 ……… (1019)
10.6 模码 ……………… (1020)
参考文献 ………………… (1022)

目　录

引言 ………………………… (1025)
1 密码学术语与概念 ……… (1025)
1.1 基本概念 …………… (1025)
1.2 信息论基础 ………… (1026)
2 对称密钥密码系统 ……… (1027)
2.1 序列密码 …………… (1027)
2.2 分组密码 …………… (1029)
3 非对称密钥密码体制 …… (1037)
3.1 RSA 公开密钥密码算法 ………………………… (1037)
3.2 Rabin 密码算法 …… (1037)
3.3 带有加密的数字签名 ………………………… (1038)
3.4 Diffie-Hellman 密钥交换体制 ………………… (1038)
3.5 DSA 美国数字签名算法 ………………………… (1039)
3.6 ElGamal 算法 ……… (1039)
3.7 背包公钥密码体制 ………………………… (1040)
3.8 McEliece 密码体制 ………………………… (1040)
3.9 基于椭圆曲线上的公开密钥密码算法 ……… (1041)
3.10 ESIGN 算法 ………… (1042)
4 散列函数 ………………… (1042)
4.1 SHA 算法 …………… (1043)
4.2 MD5 算法 …………… (1043)
4.3 基于分组密码算法的散列函数 …………… (1046)
4.4 基于离散对数的散列函数 ………………… (1046)
4.5 扩展的散列函数 …… (1046)
5 秘密分存 ………………… (1047)
5.1 沙米尔多项式插值法 ………………………… (1047)
5.2 其它门限方案 ……… (1048)
6 安全协议与密钥管理 …… (1048)
6.1 伪随机数生成 ……… (1049)
6.2 概率加密 …………… (1049)
6.3 不可否认签名 ……… (1050)
6.4 安全计算与公正掷币协议 ………………… (1051)
6.5 阈下信道 …………… (1052)
6.6 零知识证明协议 …… (1053)
6.7 量子密码 …………… (1055)
6.8 安全选举 …………… (1055)
6.9 密钥管理与分配 …… (1056)
参考文献 ………………………… (1056)